Nodes: A Network Appliance and Incentive Scheme

Justin Smith
js@xwallet.tech

Daniel Haudenschild
dhau@protonmail.com

ABSTRACT

Nodes *is an incentive-driven, consumer network appliance and software system for proprietary access to transaction broadcasting, trustless confirmation notification, payment channels, and cross chain swaps at home.*

Nodes are consumer-grade network appliances which are designed and intended to support the mass decentralization of blockchain infrastructure. The product is a pre-configured headless network computing device made in Switzerland, integrating a basic chipset, memory, internal HDD, and WiFi and Bluetooth radios. For maximum reliability and uptime, each device is equipped with an internal battery, and for convenience can act as a wireless charging station for mobile phones and other devices. Each node is pre-loaded and pre-configured to store and interact with the full blockchain for a given cryptocurrency, such as Bitcoin[1]. The nodes offer holders of digital assets the ability to access and control their cryptoassets via mobile and remote computing devices, often called ”light wallets” or ”SPV wallets”, and introduce the concept of *High Availability financial self-service* to the consumer. Second layer solutions such as the Bitcoin Lightning Network payment channel system[2], can also be used with this device. Owning two or more devices will allow cryptocurrency owners to swap cryptocurrencies without requiring the support of third parties. This enables the owners of multiple nodes to swap digital currency and cryptoassets directly, without the involvement of intermediaries, and from the comfort of home. For single device owners, each device is pre-configured with access to a proprietary trusted relay service allowing inter and intra-blockchain transactions. A novel method involving unique Augmented Reality Creatures (ARC) is used to engage and incentivize device owners to maintain their device on the network.

INTRODUCTION

Certainty that a transaction is valid in any chain is assured by the nodes which have validated the transaction block. Running your own fully validating node is the only way to ensure that 1) you can broadcast a transaction whenever you like, 2) you are using the chain you wish to use, 3) you can confirm receipt of incoming transfers. By operating a fully validating node you are also relaying the transactions of other users on the network, which is critical to the overall robustness of the network.

Today there are relatively few fully validating nodes on any given cryptocurrency network, which ultimately weakens the promise of cryptocurrency. In many cases, owners of a cryptocurrency operate a full node altruistically, or because they have a large stake in the cryptocurrency and are sufficiently aware of how critical fully validating nodes are to the overall strength of the network, directly impacting the potential value of their cryptocurrency. To operate a fully validating node which contributes significantly to the overall strength of the network, cryptocurrency users must have an uncommon degree of technical sophistication.

Many cryptocurrency users have a false sense of security in third party custodial exchanges to hold their currency on their behalf, unaware of the catastrophic failures that third party custodial exchanges have had in the past[3], and that these services are typically uninsured, are often incorporated in offshore jurisdictions, and may at any time default on their debt of cryptocurrency which is owed to the user. Block explorers and other web-based tools display information coming from a third party's node, which may not always be accurate and should never be relied on for accepting payments.

A series of high-profile losses from hacking over the years has increased awareness of the security requirements of cryptocurrency and has encouraged many users to adopt hardware wallets, where again trust in a fully validating node is outsourced to a private service provider. If the node operated by the hardware wallet service provider becomes unavailable for any reason, consumers suddenly feel betrayed, because they will not be able to broadcast transactions or see new transactions arrive until they are able to again connect to a functional node. ”Who will run the nodes?” is a serious and costly question in cryptocurrency, a cost which is currently socialized and hidden by retail investor money. Within a few years, these costs must be transferred to the users of these networks. *Nodes* is the solution.

Nodes simplifies and makes enjoyable, even enviable, the process of operating a fully validating node. There are three important conceptual aspects to the Nodes product: 1) The utility of operating your own fully validating cryptocurrency node, which makes light clients such as mobile wallets, atomic swaps, and payment channels possible 2) the bundling of a unique Augmented Reality Creature (ARC) with each network appliance, and 3) a token which is initially only available for purchase with the device and may be used to affect the ARC.

The Nodes product consists of 1) network appliance hardware pre-configured for a particular cryptocurrency 2) a companion mobile software application (CMA) for interacting with the ARC, tokens, and cryptocurrency 3) a unique ARC bundled with each new appliance sold, 4) a fixed number of tokens bundled with the hardware appliance for use with the ARC.

NETWORK APPLIANCE

The network appliance will include a simple display for viewing network statistics and hardware performance, an internal redundant power supply in the event of external power loss, wireless radios for connectivity to a home WiFi/WLAN network, and wireless charging capability for charging nearby smartphone devices on the Qi standard. Pairing the appliance to the user’s wireless network requires the user download the companion mobile application (CMA) and enter their network credentials.

Each network appliance is pre-loaded with a cryptocurrency full node, such as Bitcoin Core. The software is pre-configured, requiring no action or input from the consumer, except powering on the appliance, in order to function. Each cryptocurrency full node type will be assigned a unique ARC class, such as ”reptile”, ”mammal”, or ”fantasy”. Each appliance will ship with a random ARC belonging to the appropriate cryptocurrency class. The ARC will appear on top of the hardware device, and will be viewable with the companion mobile application (CMA). The user can interact with the ARC using tokens, a limited quantity of which will be bundled with new appliances.

Multiple network appliances will ”connect”, creating a pleasant aesthetic for display in the home. Owning multiple network appliances also affords the user additional capabilities. Cross chain atomic swaps, including layer-2 swaps[2], of the appliance’s cryptocurrencies can be conducted with other users on the network. Trading creatures for a user-defined quantity of tokens is also possible via the CMA when a consumer owns two or more appliances.

COMPANION MOBILE SOFTWARE APPLICATION (CMA)

The CMA is an interface for interacting with an ARC via tokens, interacting with cryptocurrencies, and performing basic operations related to the network appliance. The CMA experience will be the same, or very similar, on both Android and iOS operating systems. Modern hardware will be required, and the user will be asked to write down a recovery mnemonic that can be used to restore their cryptoassets in case of hardware failure.

The CMA will have an integrated order book which can be used to trade tokens, cryptocurrencies, and ARCs. Collectively, we call these cryptoassets. This order book enables two methods of trading: peer to peer (p2p) and hybrid client-server and peer to peer. Each method carries unique costs and performance characteristics. Due to the complexity of developing p2p software, early versions of the CMA will only allow hybrid trading, and true p2p trading will be available in later versions.

A viewing window in the CMA will be used to observe and interact with the ARC, which will appear to be positioned on or near the network appliance. The user may distribute tokens to the ARC in this view to elicit a reaction from the ARC.

There is a tacit link between the real world condition of the network appliance and the ARC. If network connectivity is lost, or power is lost, the ARC will be less happy than it otherwise might be. But over fixed periods of time without interruption, the ARC will happily grow and develop. Uninterrupted periods of growth for the ARC will lead to the user being rewarded with small token deposits from a special fund, for as long as said deposit fund remains liquid. While the exact dynamics of the relationship between the ARC and the user may change over time, the fundamental model is a free market economy, with a fixed supply of tokens and no inflation.

BENEFITS OF DECENTRALIZED INFRASTRUCTURE

Most cryptocurrency users today rely on third party services, including custodians, to interact with cryptoassets. Even among the most enthusiastic cryptocurrency adopters, few operate fully validating nodes. Having many nodes in a broad global distribution, rather than co-located in datacenters, means that any given cryptocurrency network will be much more resilient to a variety of attacks, including the most severe social and political attacks. The more independent nodes in operation, the more copies there are of the blockchain, and the more resilient the network.

A low number of poorly connected nodes in the network invites routing and other attacks.[4] This means that cryptocurrency owners may be blocked or restricted from exchanging their assets by an attacker, and in a worse-case scenario they may see inaccurate information when receiving payments, or they may have their transactions replayed during a hard fork. These attacks could result in a loss event.

Running your own full node is the only way to have full control of your assets and to ensure that the rules of your chosen blockchain are being followed. There are many commercial benefits that can be realized only with this decentralized approach.

SWAPPING CRYPTOASSETS A proprietary third party cryptoasset exchange provider will allow owners of a node to trade between blockchains out of the box, even if they only own one network appliance. Such an arrangement will allow the owner of a Bitcoin appliance to purchase Stellar Lumens without needing to purchase a Stellar appliance. This third party exchange service will interface with outside exchanges to provide the appropriate liquidity.

In later versions of the CMA atomic inter and intrachain swap protocols will be implemented, which will enable users to swap cryptoassets directly amongst each other. A small fee paid in cryptocurrency will be directed to the Nodes Foundation programmatically after each swap is completed.

The fee charged for the introduction of the two trading parties will generate revenue on all peer to peer transactions conducted over the protocol, a basis point model. Usage of the default third party exchange will be assessed a slightly higher fee than the atomic swap. This transaction fee revenue is paid out in the form of cryptocurrency, and this revenue represents the financial value of the network.

COLLECTING TOKENS Network appliance uptime is rewarded with tokens, which can be collected and used to interact with ARCs.

THIRD PARTY LIGHT WALLET CONNECTIVITY All third party cryptocurrency wallets with the ability to connect to a remote node may be configured to connect to the network appliance.

FUTURE DEVELOPMENT OF THE CMA The CMA is expected to develop into a multi-currency wallet with a novel distributed recovery service and multi-factor authentication options. The distributed recovery is expected to be based on a three-way authentication protocol, e.g. combinations of biometric, geographic position, and other criteria.

RESPECTING USER PRIVACY AND SOVEREIGNTY When users connect to a third-party node over the internet, sensitive data and metadata, such as the user's IP address and sometimes the transaction data, are publicly viewable and collected by potential attackers. This is true regardless of whether the node operated is trusted or untrusted. This applies to browser-based online wallets as well as for lightweight clients.

Dependence on third party nodes will never be as private, reliable, or be able to deliver the performance of your own full node.

Running a full node of the protocol you support is also an indirect way of ”voting”, and is the only way to show miners and other protocol stakeholders what rule set the owners of the network overwhelmingly support.

PREVENTING MISMATCHED RESOURCE REQUIREMENTS Publicly available nodes operated altruistically often have insufficient hardware resources for the load being placed on them. If you are unfortunate enough to try connect a light wallet to one of these nodes, you would have a zombie wallet experience, where you would be connected to the network but you cannot see incoming transactions and you cannot broadcast transactions.

CLAIMING OWNERSHIP OF FORKED COINS AND PROTECTING YOUR COINS AGAINST REPLAY ATTACKS Full nodes enforce consensus rules, and lightweight services such as wallets simply follow along with whatever full node (or group of full nodes) it is connected to. In the event of a hard fork, lightweight services will blindly follow the chain of the full node it is connected to. If you are not in control of that full node, then you are at the mercy of whoever is, and they may ultimately decide the fate of your transactions and your assets!

MULTI-CRYPTOASSET WALLET CAPABILITIES

Technology from an existing and well-adopted mobile cryptocurrency wallet which follows industry best practices[5] will be licensed into the Nodes construct. This will contribute to de-risking the project and accelerate the release of working end-to-end infrastructure. This wallet will integrate the cryptocurrency and token protocols to support network appliances.

A key function of the wallet will be to send transactions to blockchains for which the owner does not have a node. In this case the node calls a central API which allows for transactions to other currencies.

In the near future this will also include creating a swap. The wallet will also allow for monitoring of node health, and payments for Decentralized Recovery is a main usability feature of the wallet. A combination a series of tests which, when applied in combination, can eliminate false identification to a satisfactorily low number (see technical white paper).

SWAP ALGORITHM In an atomic swap protocol[6], Alice initiates a swap by creating an offer of cryptocurrency A for cryptocurrency B, and untrustworthy Bob accepts the trade. Pay to script hash and timelock contracts are used to produce signed refund transactions for both parties in the event the swap fails, such as if Bob were to attempt to cheat Alice and not deliver cryptocurrency per the terms of their swap. As such, the two parties will know each others funding UTXOs and refund transaction pubkeys at the setup stage of the protocol. This process guarantees that all swaps either complete successfully or both parties receive a full refund in the event the swap fails. This is an example of escrow-free trade, ensuring trade can safely be conducted between two untrustworthy parties at a distance without the involvement of any third party.

One key condition in an atomic swap is that both parties operate full nodes of the two cryptocurrencies being swapped. This is the only way they can ensure that they have properly validated the transactions and scripts for themselves. Otherwise, it is likely that one party could influence the outcome of the trade by attacking an outside, trusted third party.

This approach also applies generally to atomic swaps conducted via payment channels such as the Bitcoin Lightning Network.

SWAP DISCOVERY Because there is no custodial or other third party involvement in peer to peer trades, owners of network appliances will be able to trade currencies in pairs at a reduced swap rate. However, the mechanisms used to discover and communicate with peers on the network will take time to develop. In the first version of the product, swaps will by default be aggregated and processed by an external partner such as Swisscom Blockchain AG, and will be accessed via a proprietary API. This batching processes dramatically reduces the cost of discovery, and allows appliance owners to swap cryptoassets at wholesale rates. The initial variety of cryptoassets available to trade is expected to be large, with liquidity and processing managed entirely by the partner.

As swap discovery mechanisms and the liquidity of cryptoassets on the peer to peer network are improved and the technology in general matures, we expect this centralized partner will no longer be necessary.

INCENTIVE DESIGN

It’s assumed that the market for cryptocurrency full node hardware is very immature, because the market for cryptocurrency is very immature. To develop this market and train the consumer, we need to provide an incentive mechanism that the consumer can understand. Video games are something that almost everyone now understands, and in-game tokens are understood to be an effective tool for incentivizing users. The system described here is designed is to incentivize people to do two things: 1) Purchase a new hardware node and 2) Keep that hardware online. For the incentive mechanisms to be effective there must be a scarcity of token. Scarcity is created by limiting the absolute number of tokens.

The total token supply (n) is initialized and fixed at 100,000,000 for the initial production run of 1’000’000 network appliance hardware units.

How tokens are able to enter circulation and how many tokens enter circulation is expected to dramatically influence user behavior. Tokens from the total supply n will be introduced into circulation in two ways:

A) New network appliances will be bundled with tokens. Only the owner of the appliance may redeem the tokens.
B) Owners of network appliances will receive tokens for keeping their appliance online, a state which is called uptime. Downtime is the opposite state and is punished with a lower distribution coefficient, meaning the appliance owner will receive fewer, if any, tokens.

Unlike many other in-game tokens, these tokens will exist on a public blockchain. This means the tokens can be used for and in external applications, such as other games or centralized third party custodial exchanges. At launch, there will be no tokens available for sale, but there will be a buyback mechanism in place. At product launch, the Nodes Foundation will offer to purchase tokens at fixed prices in order to set the initial market price of the token.

REWARDING HARDWARE PURCHASE

To reward the purchase of new network appliance hardware, tokens will be bundled with each new appliance. These tokens can be redeemed, used with the ARC, and traded for other cryptoassets via the CMA. For the planned production run of 1’000’000 units, 30’000’000 or 30% of the total supply of tokens (n) will be bundled with new network appliance hardware.

The distribution schedule is designed such that over time fewer tokens will be bundled with new hardware in order to reward early adopters.

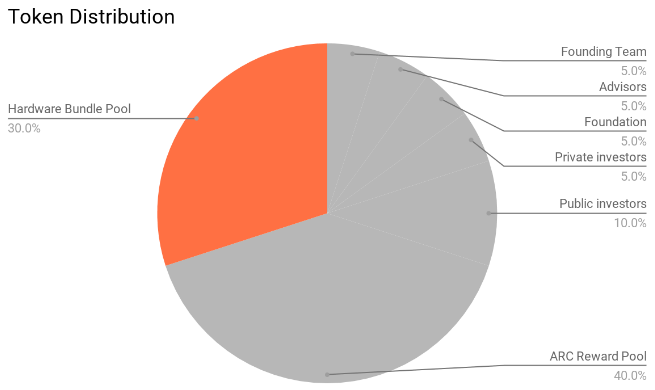


Figure 1: Quantity of tokens distributed as appliance purchase reward

Production batch	1	2	3	4
Units sold (MM)	0.001	0.01	0.05	0.1
Tokens per appliance	100	100	50	10
Tokens placed in circulation (MM)	0.1	1	2.5	1

Figure 2: Partial purchase reward distribution schedule

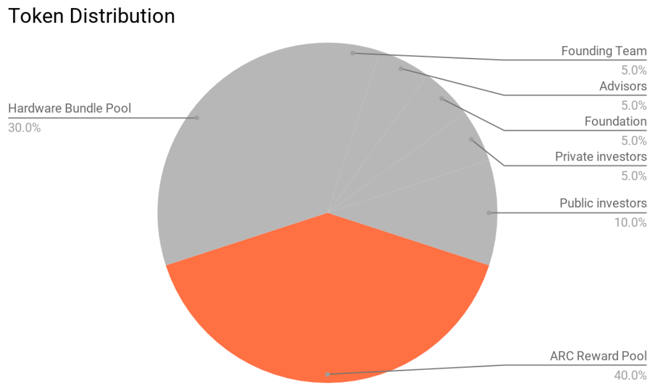


Figure 3: Quantity of tokens distributed as uptime reward

ARC REWARD POOL - REWARDING UPTIME

To strengthen the associated cryptocurrency network, network appliance uptime will be programmatically rewarded. For every 100 hours of uptime, the user will receive some amount of tokens from a fixed pool of 40'000'000 tokens (see Appendix). The payout will continue until the available supply of 40'000'000 tokens, or 40% of the total supply allocated for this purpose is reached. The distribution coefficient will vary, but in general fewer tokens will be released over time, creating an asymptotic distribution curve.

The token distribution for uptime is multiplied by a coefficient relating to ”node health”, which is a part of the gamification concept covered in the following sections. Events resulting in lower uptime (such as loss of network connectivity) is ”punished” by adversely affecting the ARC and the distribution coefficient. These events reduce the health of the ARC. The lower the ARC's health, the lower the token distribution coefficient for that node.

These two mechanisms provide a predictable way to distribute the fixed total supply tokens into circulation without giving complete certainty to the distribution outcome, which would remove the fun and interest in the game. The steady and predictable addition of a some amount of new tokens is analogous to miners expending energy and other resources to mine cryptocurrency.

ARC HEALTH AS A MEASURE OF UPTIME AND USAGE

ARCs are healthy when their associated network appliances are active on the network. When an appliance is online, the node can relay transactions, help potential cryptoasset trading partners discover each other, and of course provide a critical interface for lightweight wallets. These settings and factors are influenced by the owner, but there are a multitude of other factors and random attributes which affect the mood of the node's avatar.

Some of these attributes should be easy to discover. Exchanging cryptoassets, including ARCs, will be rewarded with a higher distribution coefficient. The health algorithm is a combination of indicators adjusted to the particular protocol, and will be different by protocol.

NURTURING AUGMENTED REALITY CREATURES (ARCS) Each network appliance unit will be bundled with a random Augmented Reality Creature (ARC). The ARC is an embodiment of the node's health and character. With the CMA, the user will be able to see the animal in AR on top of the hardware node device as the device's avatar. This avatar represents the node's overall performance and standing when compared to other nodes on the same network, and is directly tied to the token distribution coefficient.

Different classes of ARCs will be available, with each class associated with a particular cryptocurrency. For example, the class of ”Fantasy” ARCs may be bundled with Bitcoin network appliances. Within this class, a random fantasy creatures will be bundled with the network appliance. ”Reptile” might be bundled with Litecoin network appliances, etc. These ARCs can be traded using tokens, an activity which is completely under the user's control.

ARCs are ”born” with a given set of attributes and evolve in stages. Real-world events, such as power cycling the network appliance or network connectivity loss, as well as intentional user actions will impact the ARC's evolution. This means that the final form of every ARC will be relatively unique. ARCs are immortal, but evolve at different rates.

The CMA is installed on the user's personal smartphone and provides the interface used to interact with an ARC. The user's objective is to control and direct the evolution of the ARCs. During the course of the ARC's evolution, the user may choose to apply a variety of treatments, such as Vitamins, Food, Playtime, Medicine, Music, Games, Friends, and Discipline. The user may give the ARC different quantities of treatments to elicit excitement, restore health, or display a variety of other randomly selected behaviors which may last for different amounts of time based on the number of treatments which have been consumed. Each treatment carries a cost of ARC tokens. These ARC tokens are distributed to the user according to a distribution coefficient based on the number of tokens held over time by the user. These ARC tokens are distributed over time, on a predefined schedule.

When an ARC reaches its final evolutionary stage, the user will receive the highest token distribution coefficient. The ARC may be traded at any time, for any amount of tokens chosen by the user.

The overall goal of this incentive system is to increase the collectability of the network appliances and ARCs.

CONCLUSION

We have proposed a system for incentivizing consumers to take individual ownership of mission-critical financial infrastructure using a gamification technique, with the broader goal of significantly increasing the overall security and robustness of existing and future cryptocurrencies and blockchains. We expect that this project will more than triple the number of Bitcoin nodes on the network, and provide a massive boost to the decentralized nature of the blockchain and protecting the investments many have made in cryptocurrency. All while having quite a bit of fun!

REFERENCES

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[2] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf, 2016.

[3] Neuron. List of cryptocurrency exchange hacks. https://rados.io/list-of-documented-exchange-hacks/, 2018.

[4] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. https://btc-hijack.ethz.ch/files/btc_hijack.pdf.

[5] Justin Smith. Smartphone cryptocurrency wallet scorecard. https://jsmith.website/scorecard.pdf, 2018.

[6] TierNolan. Atomic cross-chain trading. https://en.bitcoin.it/wiki/Atomic_cross-chain_trading, 2013.

APPENDIX

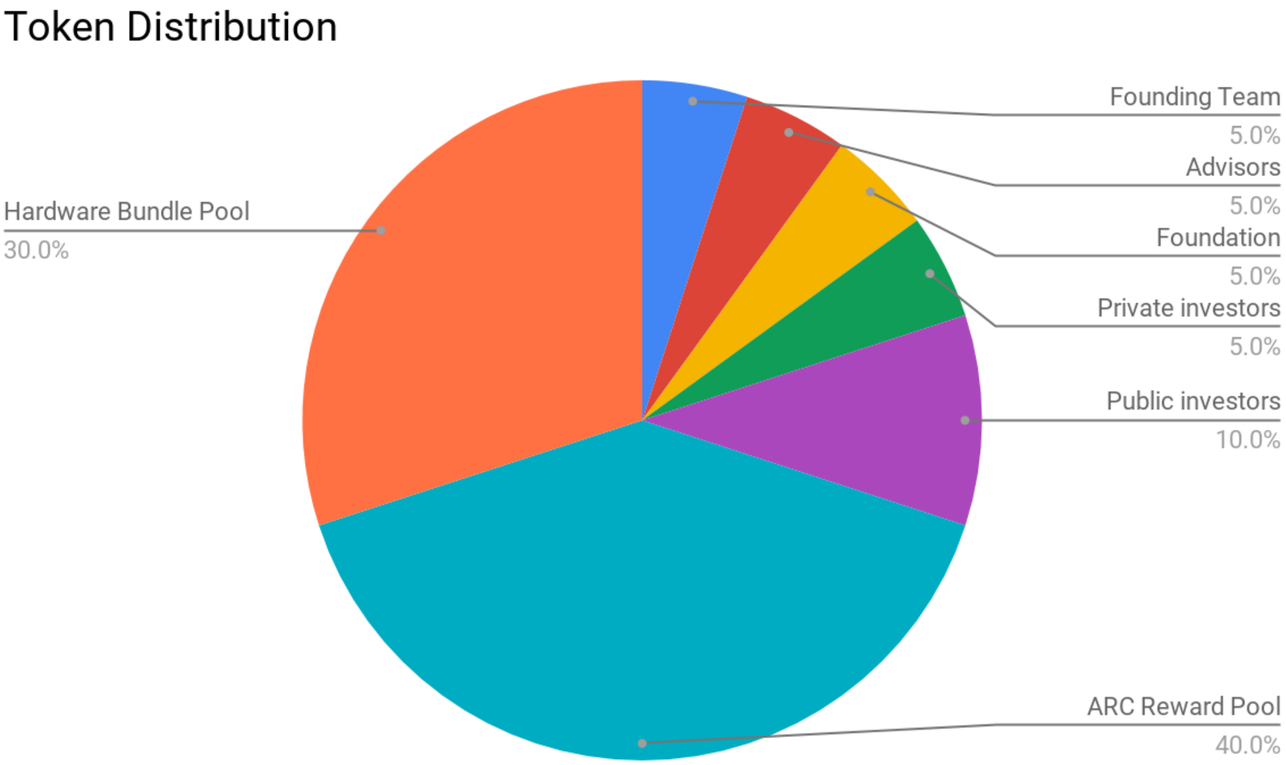


Figure 4: Token fixed supply allocation

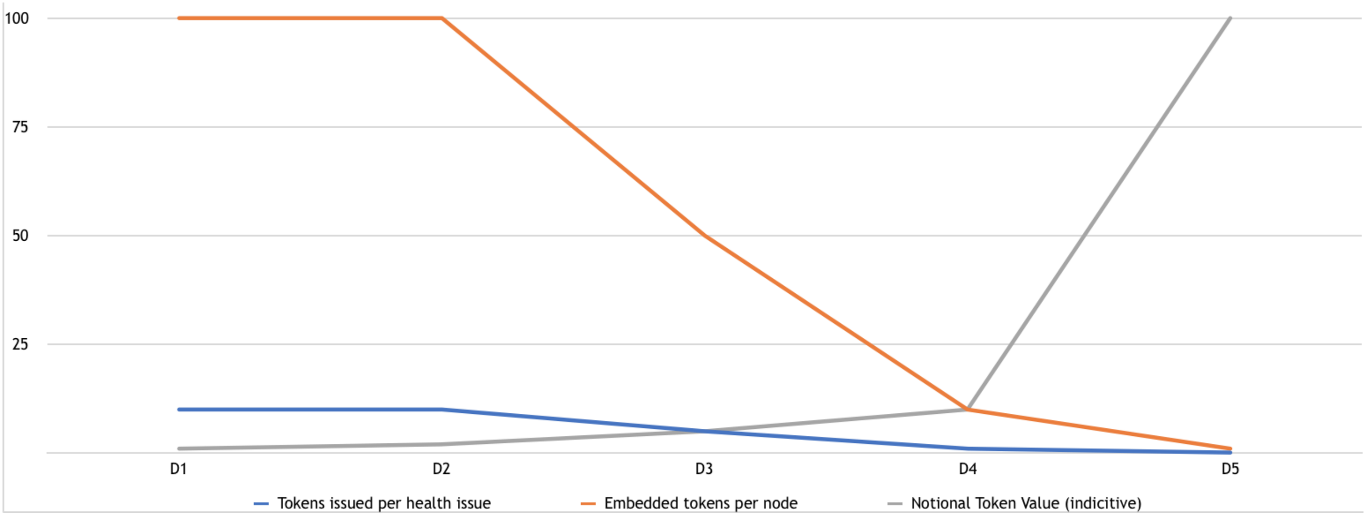
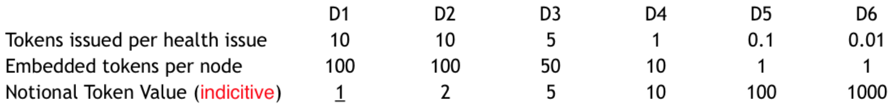
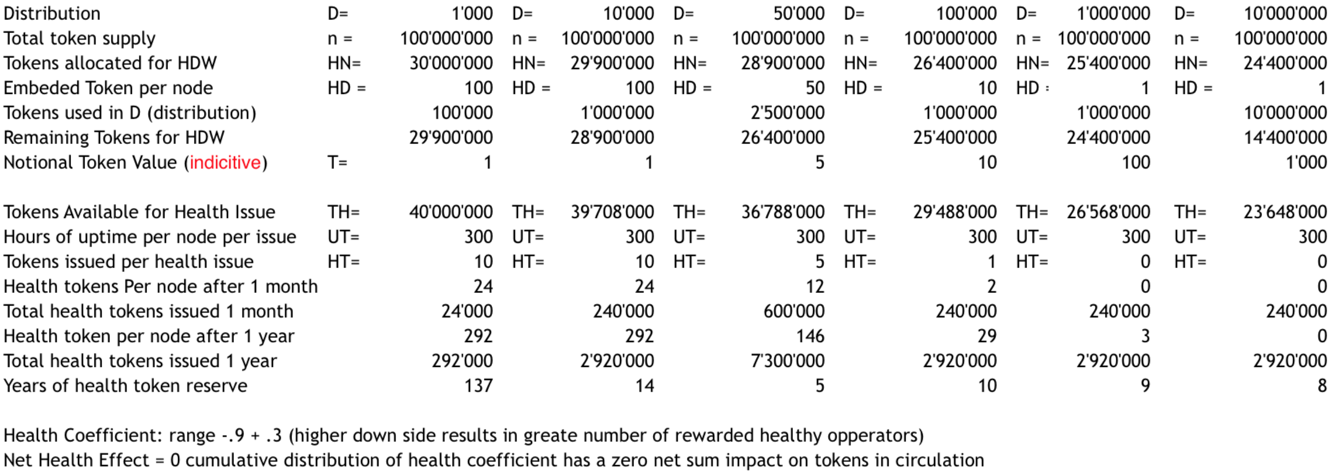


Figure 5: Plot of ARC and token distribution



	D1	D2	D3	D4	D5	D6
Tokens issued per health issue	10	10	5	1	0.1	0.01
Embedded tokens per node	100	100	50	10	1	1
Notional Token Value (indicitive)	1	2	5	10	100	1000

Figure 6: ARC and token distribution table



Distribution	D=	1'000	D=	10'000	D=	50'000	D=	100'000	D=	1'000'000	D=	10'000'000
Total token supply	n =	100'000'000	n =	100'000'000	n =	100'000'000	n =	100'000'000	n =	100'000'000	n =	100'000'000
Tokens allocated for HDW	HN=	30'000'000	HN=	29'900'000	HN=	28'900'000	HN=	26'400'000	HN=	25'400'000	HN=	24'400'000
Embeded Token per node	HD =	100	HD =	100	HD =	50	HD =	10	HD =	1	HD =	1
Tokens used in D (distribution)		100'000		1'000'000		2'500'000		1'000'000		1'000'000		10'000'000
Remaining Tokens for HDW		29'900'000		28'900'000		26'400'000		25'400'000		24'400'000		14'400'000
Notional Token Value (indicitive)	T=	1		1		5		10		100		1'000
Tokens Available for Health Issue	TH=	40'000'000	TH=	39'708'000	TH=	36'788'000	TH=	29'488'000	TH=	26'568'000	TH=	23'648'000
Hours of uptime per node per issue	UT=	300	UT=	300	UT=	300	UT=	300	UT=	300	UT=	300
Tokens issued per health issue	HT=	10	HT=	10	HT=	5	HT=	1	HT=	0	HT=	0
Health tokens Per node after 1 month		24		24		12		2		0		0
Total health tokens issued 1 month		24'000		240'000		600'000		240'000		240'000		240'000
Health token per node after 1 year		292		292		146		29		3		0
Total health tokens issued 1 year		292'000		2'920'000		7'300'000		2'920'000		2'920'000		2'920'000
Years of health token reserve		137		14		5		10		9		8

Health Coefficient: range -.9 + .3 (higher down side results in greate number of rewarded healthy opperators)

Net Health Effect = 0 cumulative distribution of health coefficient has a zero net sum impact on tokens in circulation

Figure 7: Detail ARC reward ("health") and token distribution